The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/22/2020

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Mozilla Firefox ESR, the most severe of which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Mozilla Firefox versions prior to 81
- Mozilla Firefox ESR versions prior to 78.3

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- By exploiting an Open Redirect vulnerability on a website, an attacker could have spoofed the site displayed in the download file dialog to show the original site (the one suffering from the open redirect) rather than the site the file was actually downloaded from. (CVE-2020-15677)
- Memory safety bugs are present in Firefox 80 and Firefox ESR 78.2. Some of these bugs showed evidence of memory corruption and it is presumed that with enough effort some of these could be exploited to run arbitrary code. (CVE-2020-15673)
- When recursing through graphical layers while scrolling, an iterator may have become invalid, resulting in a potential use-after-free. This occurs because the function APZCTreeManager::ComputeClippedCompositionBounds did not follow iterator invalidation rules. (CVE-2020-15678)
- Firefox sometimes ran the onload handler for SVG elements that the DOM sanitizer decided to remove, resulting in JavaScript being executed after pasting attacker-controlled data into a contenteditable element. (CVE-2020-15676)
- A Use-After-Free vulnerability exists in WebGL such that when processing surfaces, the lifetime may outlive a persistent buffer leading to memory corruption and a potentially exploitable crash. (CVE-2020-15675)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2020-42/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-43/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15673
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15675
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15676
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15677
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15678